IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
ASHEVILLE DIVISION

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE GOOGLE ACCOUNT BRIANASLEEPZ123@GMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC	Case No. 1:22-mj-00027 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Alicia Boppe, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with the Google Gmail account, brianasleepz123@gmail.com ("the Account") that is stored at premises owned, maintained, controlled, or operated by Google LLC ("Google"), an electronic communications service and/or remote computing service provider headquartered at 1600 Amphitheater Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation and have been since May 2018. As a Special Agent with the FBI, I have managed investigations into criminal

and counter-intelligence matters, conducted interviews, evidence searches, surveillances, arrest operations, electronic monitoring, and general investigative research. I have continued my professional education through in-service and online courses, to include counter-intelligence, case management, operation of confidential sources, and investigative research methods. Prior to joining the FBI, I worked as the Director of Environmental Health ,Safety and Regulatory Affairs for a chemical manufacturing company. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws and I am authorized by the Attorney General to request a criminal complaint and arrest warrant.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and distribute child pornography); 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography) involving the use of a computer and the Internet, is located in and within the aforementioned account. I have probable cause to believe that the member account that is the subject of this application will have stored information and communications that are relevant to this investigation, including evidence of the identity of the person maintaining the account associated with "the Account". Based on my training and experience, there is probable cause to believe that evidence, fruits and/or instrumentalities of the aforementioned crimes are located in the account.

5. The statements contained in this Affidavit are based in part on information provided by other law enforcement officers; written reports about this and other investigations that I have

received, information gathered from the service of administrative subpoenas; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent with the FBI. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and distribute child pornography); 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography), have been committed by the person or persons who used the Google account brianasleepz123@gmail.com.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).]

DEFINITIONS

7. The following definitions apply to this Affidavit:

a) "Child Pornography" and "Child Sexual Abuse Material" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital

image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

b) "Sexually explicit conduct" refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, anal-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2) (A).

c) "IP Address" or Internet Protocol address is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

d) "Computer" refers to an electronic, magnetic, optical, electrochemical, or other highspeed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e) (1).

e) "The Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

8. Based on my training, experience and knowledge, I know the following: Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and used. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). To distribute these on any scale, it required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these was accomplished through a combination of personal contact, mailings, and telephone calls.

9. The development of computers has added to the methods used by collectors of child pornography to interact with, and sexually exploit, children. Computers serve four functions in connection with child pornography: production, communication, distribution, and storage.

10. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

11. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Electronic Service Providers, such as Google, as well as remote storage accounts like Dropbox, Google Drive, mega.nz, cloud.mail.ru, puc.upload.de, and Yandex Disk. These online services allow a user to set up an account with a remote computing or storage services of computer files in a variety of formats.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

12. Based on my experience, training, and conversations with other experienced law enforcement officers who investigate cases involving the sexual exploitation of children, I know

that certain common characteristics are often present in individuals who collect child pornography including the following:

a. Many individuals who traffic in and trade images of child pornography also collect child pornography. Many individuals who collect child pornography have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by sexually explicit depictions of children.

b. Many individuals who collect child pornography often seek out like minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance, and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest and associated behavior.

13. Based upon my training and experience, as well as my conversations with other experienced law enforcement officers, I know that individuals who collect and trade child pornography often do not willfully dispose of their child pornography collections, even after contact with law enforcement officials.

14. Individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage to their collection of illicit materials. The known desire of such individuals to retain child pornography together with the sense of security afforded by using computers, provides probable cause to believe that computer images, especially child pornography and erotic nudity involving minors, will be retained by the collector indefinitely. These individuals may protect their illicit materials by passwords, encryption, and other security measures, save it on movable media such as CDs, DVDs, flash memory, thumb drives, and removable hard drives,

which can be very small in size, including as small as a postage stamp, and easily secreted, or save it to storage sites via the Internet.

BACKGROUND CONCERNING GOOGLE[1]

15. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

16. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

17. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

[1] The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the "Google legal policy and products" page available to registered law enforcement at lers.google.com; product pages on support.google.com; or product pages on about.google.com.

18. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

19. Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses ("recovery," "contact," "forwarding," or "alternate" email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

20. Google provides an address book for Google Accounts through Google Contacts. Google Contacts stores contacts added by the user, as well as contacts the user has interacted with in Google products, up to 25,000 contacts. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their Android device address book with their account so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them. Contacts can be accessed from the same browser window as other Google products like Gmail and Calendar.

21. Google provides an appointment book for Google Accounts through Google Calendar, which can be accessed through a browser or mobile application. Users can create events or RSVP to events created by others. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and

auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their device calendar so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the user deletes them. Calendar can be accessed from the same browser window as other Google products like Gmail and Calendar.

22. Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the messages, though other factors may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.

23. Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to Google Drive. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment.

Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me." Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

24. Google Keep is a cloud-based notetaking service that lets users take notes and share them with other Google users to view, edit, or comment. Google Keep notes are stored indefinitely, unless the user deletes them.

25. Google offers a cloud-based photo and video storage service called Google Photos. Photos and videos can be shared with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.

26. Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-by-turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. Users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.

27. Google collects and retains data about the location at which Google Account services are accessed from any mobile device. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Precision location data is typically stored by Google in an account's Location History and is assigned a latitude-longitude coordinate with a meter radius margin of error. Inferential data is stored with an account's Web & App Activity. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen months. Accounts created after June 2020 auto-delete Location History and Web & App Activity after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

28. Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account in a record called My Activity.

29. Google also offers a video platform called YouTube that offers Google Accounts the ability to upload videos and share them with others. Users can create a YouTube channel where they can upload videos, leave comments, and create playlists available to the public. Users can subscribe to the YouTube channels of others, search for videos, save favorite videos, like videos, share videos with others, and save videos to watch later. More than one user can share control of a YouTube channel. YouTube may keep track of a user's searches, likes, comments, and change history to posted videos. YouTube also may keep limited records of the IP addresses used to access particular videos posted on the service. Users can also opt into a setting to track their YouTube Watch History. For accounts created before June 2020, YouTube Watch History is stored indefinitely, unless the user manually deletes it or sets it to auto-delete after three or eighteen months. For accounts created after June 2020, YouTube Watch History is stored for three years, unless the user manually deletes it or sets it to auto-delete after three or eighteen months.

30. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a

user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

31. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

32. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

33. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

34. In my training and experience, evidence of who was using a Google account and from where, as well as evidence related to criminal activity of the kind described above, may be

found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

35. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation.

36. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

37. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators or victims. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of additional victims and instrumentalities of the crimes under investigation.

38. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my

training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

PROBABLE CAUSE AND DETAILS OF THE INVESTIGATION

39. In approximately March 2020, the FBI Minneapolis office began investigated a particular subject ("Subject 1") who was using multiple Google Gmail accounts and other similar services to advertise, receive, and distribute child pornography.

40. In October 2020, FBI Minneapolis received records from Google LLC in response to a District of Minnesota search warrant for the contents of one of Subject 1's Gmail accounts, saraashley009@gmail.com.

41. Review of the contents of the saraashley009@gmail.com Gmail account revealed that Subject 1 communicated with another Gmail user, brianasleepz123@gmail.com, display name "Briana Stevens," from approximately June 20, 2019, until approximately May 6, 2020. The emails had a subject line of "Trade Still" and contained multiple links connected to cloud storage.

42. Email communications between saraashley009@gmail.com and brianasleepz123@gmail.com involved discussions concerning the exchange of images and videos of child pornography. Some examples include the following:

> **12/12/2019** - from saraashley009@gmail.com to brianasleepz123@gmail.com
>
> Body: [Links to Google Drive, mega.nz, and Dropbox.] [The Google Drive was publicly viewable at the time FBI Minneapolis reviewed the account. The folder contained sexually explicit images and videos depicting children under the age of 18 and adult females.]
>
> **12/12/2019** - from brianasleepz123@gmail.com to saraashley009@gmail.com
>
> Body: Only I like hardcore . dad n daughter or 4 to 11 yo with man . with sound . possible rape u have ? O i have a few more links

3/5/2020 - to brianasleepz123@gmail.com from saraashley009@gmail.com

Body: [Six links to Yandex Disk folders and one link each to mega.nz, Google Drive, and Dropbox folders. Two of the Yandex Disk links were active at the time FBI Minneapolis reviewed it and contained child pornography files, including images of very young children engaged in sexual contact with adult men and girls approximately 11-12 years of age in poses of sexually explicit nudity.]

3/5/2020 - from brianasleepz123@gmail.com to saraashley009@gmail.com

Body: I'm not sure any work . haven't looked haven't looked at yours ..... Here though Also do u have any hardcore rape videos with sound girl and man . [15 links to mega.nz folders]

3/5/2020 - to brianasleepz123@gmail.com from saraashley009@gmail.com

Body: Ya none of those work

3/5/2020 - from brianasleepz123@gmail.com to saraashley009@gmail.com

Body: Sorry here [one link each to mega.nz and cloud.mail.ru folders.]

4/24/2020 - to brianasleepz123@gmail.com from saraashley009@gmail.com

Body: [four links to mega.nz folders and one link each to Yandex Disk, Dropbox, and Google Drive folders.]

5/6/2020 - from brianasleepz123@gmail.com to saraashley009@gmail.com

Body: [Three links to mega.nz folders and one link each to Dropbox, cloud.mail.ru, and puc.upload.de folders]

43. In August 2021, Subject 1 pled guilty to the distribution of child pornography in the United States District Court for the District of Minnesota.

44. On December 6, 2021, Google LLC provided FBI Minneapolis records responsive to an administrative subpoena for information associated with the Google account, brianasleepz123@gmail.com. Google records reflected the following information associated with that Gmail account:

Name: Briana Stevens
Created on: 2018-09-16 03:12:26 UTC
Services: Gmail, Web & App Activity, Location History, Android, Google Calendar,

YouTube, Google Keep
Recent IPs:

67.21.183.222 2021-11-30 02:05:35 UTC [TruVista Communications, Toccoa, GA]

Verizon Wireless

174.250.176.98 2021-11-23 00:41:26 UTC
174.215.134.171 2021-11-16 01:38:43 UTC
174.250.180.85 2021-11-09 02:50:13 UTC

Hughes Net

2001:5b0:211f:9ac8:6870:7c08:160f:321a 2021-11-19 04:11:49 UTC

45. On December 8, 2021, Hughes Network Systems, an Internet service provider, provided records responsive to an administrative subpoena sent by FBI Minneapolis for information associated with the Hughes Network Systems account assigned the IP address 2001:5b0:211f:9ac8:6870:7c08:160f:321a on November 19, 2021, at 04:11:49 UTC. Hughes Network Systems records reflected the following information:

Device/Site ID: DSS200952620
Site Contact Name: Nathan Griffith
Site Address: 7025 Old Fort Sugar Hill Rd., Marion, NC 28752-6969
Phone: 828-803-4661
Email: griffithaintingnc@gmail.com
Billing Address: 840 Stoney Stream Ln., Arden, NC 28704-9113
Account Creation Date: 06/07/2021

46. On December 8, 2021, TruVista Communications provided records responsive to an administrative subpoena sent by FBI Minneapolis for information associated with the TruVista Communications account assigned the IP address 67.21.183.222 on November 30, 2021, at 0:05:35 UTC. TruVista Communications records reflected the following:

Subscriber Name: TOCCOA INN AND SUITES
Subscriber & Billing Address: 106 STEPHENS CIR TOCCOA, GA 30577
Acount Activation Date: 06/23/2017

Account Deactivation Date: Account is still active
Associated Phone Numbers: 770-757-5902

47. On December 27, 2021, Verizon Wireless provided records responsive to an administrative subpoena sent by FBI Minneapolis for information associated with IP addresses 174.250.176.98; 174.215.134.171; and 174.250.180.85 used to access brianasleepz123@gmail.com. Verizon records reflected the following information about the wireless account associated with those IP addresses:

Subscriber: TracFone
Telephone number: 828-230-9871
Effective: 6/5/2021
Device IMEI: 357263230419635
Device IMSI: 311480618552207
Device Type: SM-S102DL Samsung Galaxy A10e

48. On March 17, 2022, TracFone provided records responsive to an administrative subpoena sent by FBI Minneapolis for information associated with telephone number 828-230-9871. TracFone records reflect the following information concerning that account:

Name: None Provided
Email: scottnations743@gmail.com
Date of Birth: 5/7/1991
Device Serial: 357263230419635
Purchase Date: 9/30/2021
Billing Name: Scott Nelson
Credit Card: -5018, exp 6/2025
Address: 7025 Old Fort, Marion, NC 28752

49. FBI Minneapolis conducted a public record search and located an individual named Scott Demas NATIONS, date of birth, May 7, 1991, who was a resident of 7025 Old Fort Sugar Hill Road, Marion, NC 28752. The listed address was the same as the subscriber address

for IP addresses that had accessed the brianasleepz123@gmail.com Google account was registered to Hughes Network Systems.

50. On March 12, 2020, FBI Minneapolis submitted a preservation request for Google account brianasleepz123@gmail.com.

51. On March 18, 2022, FBI Minneapolis sent a lead to the FBI Charlotte Field Office- Asheville Resident Agency regarding the child pornography investigation into the Google account brianasleepz123@gmail.com.

52. On April 7, 2022, your affiant reviewed information received from FBI Minneapolis and observed that the Google account brianasleepz123@gmail.com had sent and received child pornography including the following:

a. On or about December 12, 2019, brianasleepz123@gmail.com sent a Google Drive link to another Google user that contained explicit material including a video depicting a female approximately 12-14 years old displaying her genitals in a lewd and lascivious manner.

b. On or about March 5, 2020, brianasleepz123@gmail.com received a Yandex.disk link containing a folder labeled "Courtney (2009)" which contained images of an adult male digitally rubbing the vagina of a prepubescent female and performing oral sex on the same prepubescent female. Within the same link was a folder named "12yo Girl & Sex Toys" which contained images of a naked female approximately 12 years old inserting objects into her vagina and anus.

53. On April 10, 2022, an investigation was opened by the FBI Asheville Resident Agency.

54. On April 25, 2022, FBI Asheville submitted a preservation request to Google for the account brianasleepz123@gmail.com.

55. On May 2, 2022, FBI Asheville submitted an administrative subpoena to Google for subscriber information associated with the brianasleepz123@gmail.com Google account.

56. On May 2, 2022, Google responded to the administrative subpoena with the following information:

Google Account ID: 200634719672
Name: Briana Stevens
Given Name: Briana
Family Name: Stevens
e-Mail: brianasleepz123@gmail.com
Alternate e-Mails:
Created on: 2018-09-16 03:12:26 Z
Terms of Service IP: 174.255.128.40
Services: Gmail, Location History, Android, Google Calendar, YouTube, Google Keep
Deletion Date:
Deletion IP:
End of Service Date:
Last Updated Date: 2022-04-17 22:03:32 Z
Last Logins: 2022-04-17 22:03:32 Z, 2022-04-13 01:23:24 Z, 2022-04-06 23:37:55 Z

57. Based on the information received from Google, your affiant confirmed the email account brianasleepz123@gmail.com is still an active account, with the last login on April, 17, 2022.

CONCLUSION

58. Based on the forgoing, I request that the Court issue the proposed search warrant.

59. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then

compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

60. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Reviewed by Assistant United States Attorney Alexis Solheim.

/S/ Alicia Boppe
Date: May 10, 2022
Special Agent
Federal Bureau of Investigation

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this 10th day of May, 2022, at 3:14 PM.

Signed: May 10, 2022

W. Carleton Metcalf
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with brianasleepz123@gmail.com ("the Account") that is stored at premises owned, maintained, controlled, or operated by Google LLC a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC ("Google")

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on April 25, 2022 with the Google Reference Number 16672840 and 3579523, Google is required to disclose to the government for each account or identifier listed in Attachment A the following information from **June 20, 2019 to Present** unless otherwise indicated:

a. All business records and subscriber information, in any form kept, pertaining to the Account, including:

1. Names (including subscriber names, user names, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);
3. Telephone numbers, including SMS recovery and alternate sign-in numbers;
4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, including log-in IP addresses;
5. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers
6. Length of service (including start date and creation IP) and types of service utilized;
7. Means and source of payment (including any credit card or bank account number); and

8. Change history.

b. All device information associated with the Account, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;

c. Records of user activity for each connection made to or from the Account(s), including, for all Google services, the date, time, length, and method of connection, data transfer volume, user names, source and destination IP address, name of accessed Google service, and all activity logs

d. The contents of all emails associated with the ACCOUNT, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails;

e. Any records pertaining to the ACCOUNT's contacts, including: address books; contact lists; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history;

f. Any records pertaining to the ACCOUNT's calendar(s), including: Google Calendar events; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history;

g. The contents of all text, audio, and video messages associated with the ACCOUNT, including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history;

h. The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes and note titles, lists, [ANDROID USER: applications], and other data uploaded, created, stored, or shared with the account including drafts and deleted records; [ANDROID USER: third-party application data and backups]; [SMS data and device backups]; the creation and change history of each record;

accounts with access to or which previously accessed each record; any location, device, other Google service (such as Google Classroom or Google Group), or third-party application associated with each record; and all associated logs, including access logs and IP addresses, of each record;

i. The contents of all media associated with the ACCOUNT in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses;

j. All maps data associated with the ACCOUNT, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; My Maps data; accounts and identifiers receiving or sending Location Sharing information to the account; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history;

k. All Location History and Web & App Activity indicating the location at which the ACCOUNT was active, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car), and associated logs and user settings, including Timeline access logs and change and deletion history;

l. All Internet search and browsing history, and application usage history, including Web & App Activity, Voice & Audio History, Google Assistant, and Google Home, including: search queries and clicks, including transcribed or recorded voice queries and Google Assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history;

m. Records associated with the ACCOUNT's YouTube registration, including the ACCOUNT's display name, IP logs, channel ID, account registration information, and registration email;

n. The contents of all media associated with the ACCOUNT on YouTube, whether active, deleted, or in draft, including: copies of videos and other media only if uploaded to, saved to, shared by or shared with the account; playlists; connected applications; associated URLs for each record; creation and change history;

privacy settings for each record; and all associated logs, including IP addresses, locations, timestamps, and device identifiers;

Google is hereby ordered to disclose the above information to the government within **14** days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and distribute child pornography); 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography) those violations involving "the Account" and occurring from June 20, 2019 to Present, including, for each Account or identifier listed on Attachment A, information pertaining to the following matters:

a. Evidence of violations of 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and distribute child pornography); 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography)

b. Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

c. Evidence indicating the Account owner's state of mind as it relates to the crime under investigation;

d. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed

electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google LLC ("Google"), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, and they were made by Google as a regular practice; and

b. such records were generated by Google's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature